



**UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/979,983	11/26/97	MICALI	S MIM-022.04

LM02/0524

PATENT GROUP
HUTCHINS, WHEELER & DITTMAR
101 FEDERAL STREET
BOSTON MA 02110

EXAMINER

KABAKOFF, S

ART UNIT	PAPER NUMBER
----------	--------------

2767

20

DATE MAILED:

05/24/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.

08/979,983

Applicant(s)

MICALI, SILVIO

Examiner

Steve Kabakoff

Art Unit

2767

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

- 1) ☒ Responsive to communication(s) filed on 24 March 1998.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 83-163 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 83-163 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).
- a) ☐ All b) ☐ Some * c) ☐ None of the CERTIFIED copies of the priority documents have been:
- ☐ received.
 - ☐ received in Application No. (Series Code / Serial Number) _____.
 - ☐ received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

- 15) ☒ Notice of References Cited (PTO-892)
- 16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 17) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4,6-9,15, 17,18
- 18) ☐ Interview Summary (PTO-413) Paper No(s). _____
- 19) ☐ Notice of Informal Patent Application (PTO-152)
- 20) ☒ Other: office action for 09/028, 535
- 21) ☒ other claims, grounds and reasons for allow in 08/729619

Art Unit: 2767

DETAILED ACTION

1. Claims 83-163 have been examined.

The applicant canceled claims 1-82 in preliminary amendments.

Double Patenting

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. Claims 83-163 are provisionally rejected under the judicially created doctrine of double patenting over the claims of copending Application No. 08/729619 titled "Tree-Based Certificate Revocation System" which was allowed October 1, 1999 by Examiner Sayadian. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows:

Claims 83-163 in the instant application are directed towards methods for an intermediary to prove to an end user that certificate information is authenticated by an authority

Art Unit: 2767

in a manner that enables the end user to verify portions of the information using authenticated tree data structures containing the certificate information.

Copending Application No. 08/729619 titled "Tree-Based Certificate Revocation System" which was allowed October 1, 1999 by Examiner Sayadian teaches the same methods as the instant application for an intermediary to prove to an end user that certificate information is authenticated by an authority using authenticated tree data structures; in particular, the examiner refers the applicant to claim 13 and part (b) of claim 1 in allowed application 08/729619 (note that allowed claim 13 was originally filed as claim number 71).

Furthermore, in the "Examiner's Statement of Reasons for Allowance" for copending Application No. 08/729619, Examiner Sayadian identified the patentable feature of the allowed claims to be an entity other than the certification authority (ie, an intermediary) using authenticated tree data structures to prove to an end user that certificate information, such as revocation information, is authenticated by an authority:

"The cited prior art, neither alone nor in combination, teaches or suggests the limitations of an entity other than the certification authority constructing at least one Merkle Tree [a type of authenticated tree data structure] containing on its nodes the plurality of values indicating the certificates that have been revoked, as now recited in the independent claims." [emphasis added]

There is no apparent reason why the applicant would be prevented from presenting claims corresponding to those of the instant application in the other copending application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

4. Claims 83-163 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 39, 40, 42-47 of copending Application No. 09/028535 in view of Micali (US 5666416).

Copending Application No. 09/028535 teaches using authenticated tree data structures, such as Merkle Trees, containing certificate information to prove to an end user that the certificate information stored in the tree data structures is authenticated by an authority in a manner that allows the end user to verify portions of the information.

Copending Application No. 09/028535 differs from the instant application since it does not disclose the use of an intermediary.

However, throughout the disclosure of Micali (US 5666416) a directory is disclosed (ie, see abstract and Fig. 1 in Micali (US 5666416)) that stores authentication information and acts as an intermediary between an authority and an end user. Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention in possession of Micali (US 5666416) to combine the claimed methods in copending Application No. 09/028535 with the directory structure taught in Micali (US 5666416) since the directory acts as an intermediary buffer between the end user and a certification authority and can effectively dispense individualized certificate information requested by an end user within a large network environment.

This is a provisional obviousness-type double patenting rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2767

6. Claims 83-163 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brands (US 5606617), Merkle (US 4309569), Perlman et al (US 5687235), and page 2, line 14 through page 4, line 2 of the instant specification.

As mentioned in the double patenting rejection in paragraph 4 above, the claimed inventions teach the same methods disclosed in copending Application No. 09/028535 which was rejected based on the following:

- A) It was known at the time of the invention to store certificate information about a plurality of public keys in a tree data structure (Brands (US 5606617)).
- B) Merkle Trees and their advantages as a tree data structure were well known at the time of the invention (Merkle (US 4309569)).
- C) Storing certificate revocation information in a data structure was well known at the time of the invention (Perlman et al (US 5687235)).

The examiner refers the applicant to the Office Action mailed to him on March 16, 2000 in regards to copending Application No. 09/028535 which explains why one of ordinary skill in the art would know to combine Brands (US 5606617), Merkle (US 4309569), and Perlman et al (US 5687235) to disclose the inventions claimed in copending Application No. 09/028535. The examiner has listed this Office Action ^{as an attachment} ~~on the current PTO-892~~ as well as in the "Prior Art Made of Record" in paragraph 7 below.

As mentioned in the previous double patenting rejections, claims 83-163 in the present application teach the additional limitation of the use of an intermediary which is not taught in copending Application No. 09/028535. However, the examiner asserts the instant specification discloses that the benefits of using an intermediary directory was well known and often practiced in the art at the time of the invention and would be an obvious addition to the

B
5-19-00

Art Unit: 2767

combined method of Brands (US 5606617), Merkle (US 4309569), and Perlman et al (US 5687235):

D) On page 2, line 14 through page 4, line 2 of the instant specification, the applicant concedes the use of an intermediary (or "directory") was well known in the art at the time of the invention as a means for dispensing certificate revocation information to an end user

It would have been obvious to one of ordinary skill in the art at the time of the invention to include a directory, as the applicant concedes was known in the art at the time, in the combined system of Brands (US 5606617), Merkle (US 4309569), Perlman et al (US 5687235) since a directory acts as an intermediary buffer between the end user and a certification authority and can effectively dispense individualized certificate information requested by an end user within a large network environment.

Therefore, claims 83-163 are rejected in view of the combination of points (A), (B), (C), and (D) above.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure and attachments.

- Leighton (US 5432852)
- Kocher (US 5903651)
- Office Action for copending Application No. 09/028535 (Attachment)
- Claims, amendments, and Reason for Allowance for copending (Attachment)

Application No. 08/729619

B
5-19-00

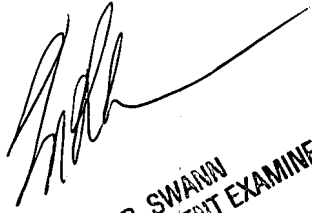
Art Unit: 2767

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steve Kabakoff whose telephone number is (703) 306-4153. The examiner can normally be reached on 8:30am to 6:00pm except every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on (703) 308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 305-9051 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

SK
SEK
May 17, 2000



TOD R. SWANN
SUPERVISORY PATENT EXAMINER
GROUP 2700